Achieving a High Level of Rigor in Using Software For WIPP

Gary K. Froehlich

Nuclear Waste Management Programs

Regulatory Compliance Department 6821

phone: (505)284-3930

e-mail: gkfroeh@Sandia.gov

Sandia National Laboratories

Achieving a High Level of Rigor in Using Software For WIPP -- Contents 1

- Description of WIPP
- SNL's Role in WIPP
- Performance Assessment
- Origins of Our QA Requirements
- The Requirements, Summarized
- Our Definition of "a High Level of Rigor"
- Application of Our Definition
- Where We Began
- Implementation of Software QA
- SQA Documentation

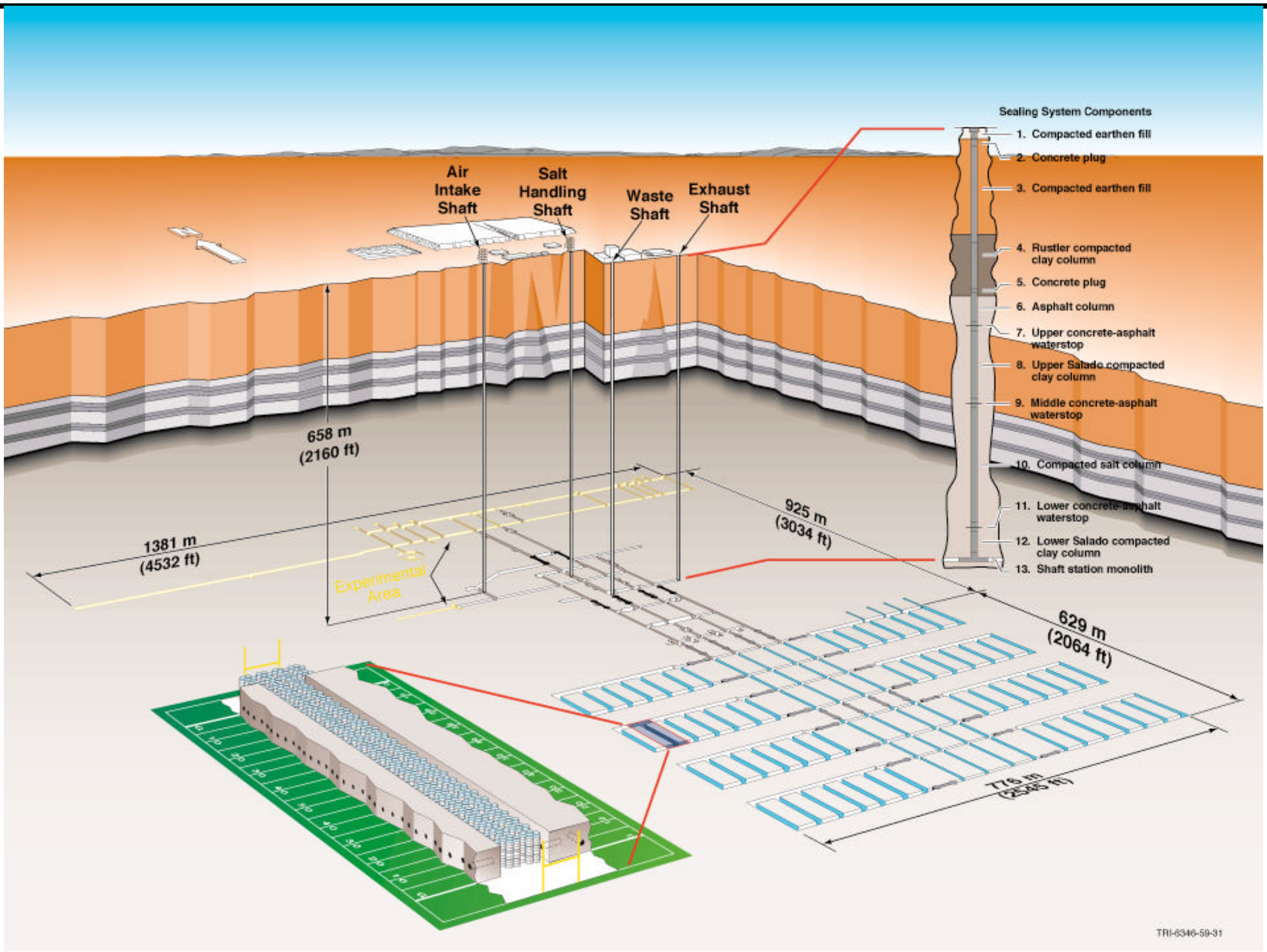
Achieving a High Level of Rigor in Using Software For WIPP -- Contents 2

- SQA -- Benefits
- Our Definition of Software Management System (SMS)
- Implementation of SMS
- Our Definition of Run Control
- Implementation of Run Control
- SMS and Run Control -- Benefits
- How Well it All Worked
- Lessons Learned
- What Next?

The Waste Isolation Pilot Plant -- WIPP

- The Department of Energy's (DOE) WIPP is a deep geologic repository for the permanent disposal of transuranic (TRU) waste
- It is the first such repository in the United States to have successfully demonstrated compliance with the US Environmental Protection Agency's (EPA) long-term radioactive waste disposal requirements
- First disposal of TRU waste at WIPP occurred on March 26, 1999

Cutaway Schematic of the WIPP


Air Intake Shaft
Salt Handling Shaft
Waste Shaft
Exhaust Shaft
658 m (2160 ft)
1381 m (4532 ft)
925 m (3034 ft)
629 m (2064 ft)
776 m (2545 ft)
Experimental Area
Sealing System Components
1. Compacted earthen fill
2. Concrete plug
3. Compacted earthen fill
4. Rustler compacted clay column
5. Concrete plug
6. Asphalt column
7. Upper concrete-asphalt waterstop
8. Upper Salado compacted clay column
9. Middle concrete-asphalt waterstop
10. Compacted salt column
11. Lower concrete-asphalt waterstop
12. Lower Salado compacted clay column
13. Shaft station monolith
TRI-6346-59-31

SNL's Role in WIPP

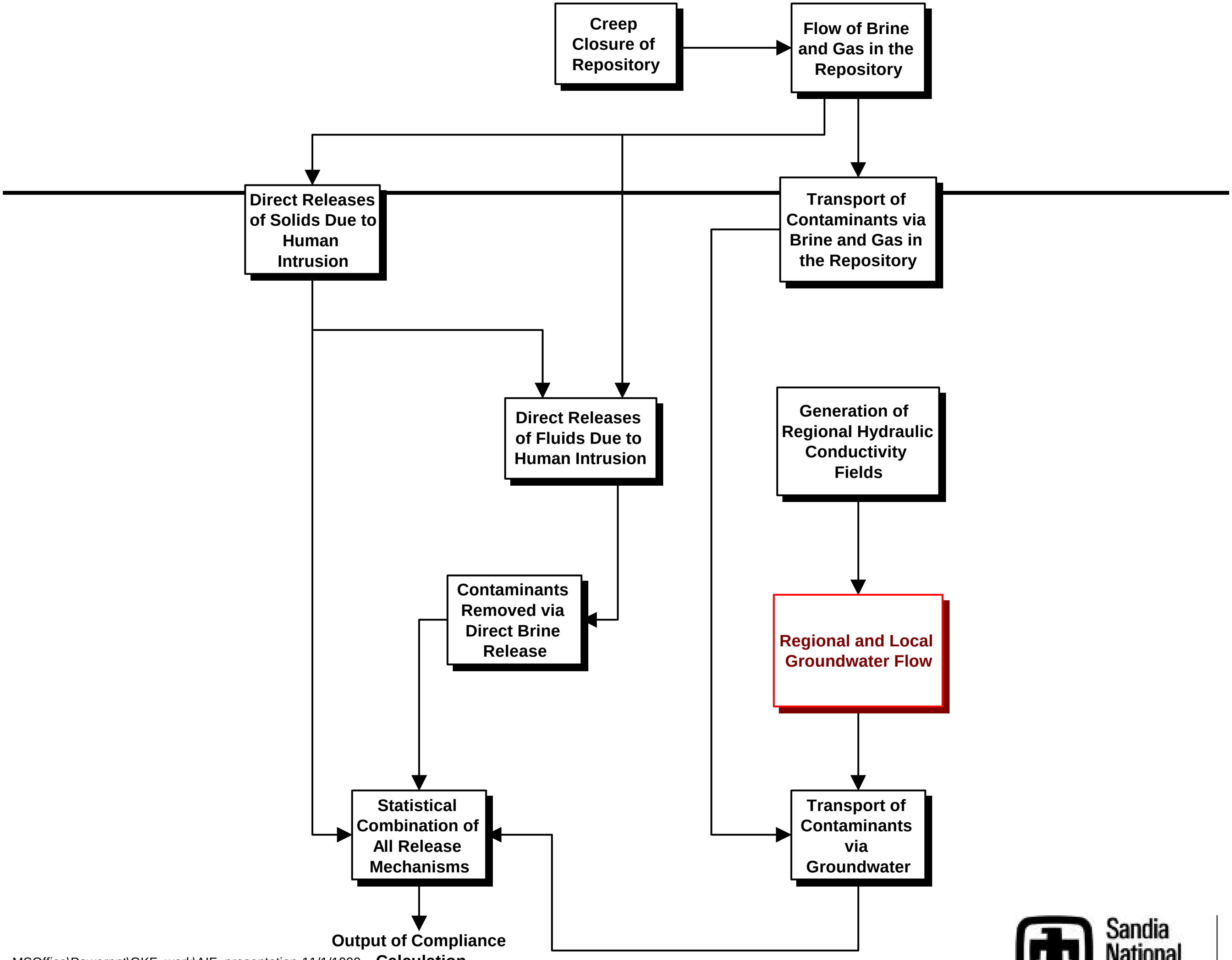
- Science Advisor to the DOE
- Teamed with:
  - DOE Carlsbad Area Office (CAO)
  - Westinghouse Electric Corp. (WID)
- Responsibilities included:
  - Data collection, site characterization, model development
  - System Prioritization -- a determination of the relative importance of scientific activities with respect to their impact on regulatory compliance
  - Performance Assessment (PA) -- a risk-based analysis of whether the repository will perform as expected over its 10,000-year containment period

Performance Assessment for WIPP - 1

- Characterization of the repository system
  - Interpretation of field and lab data to describe site-scale phenomena
  - Modeling of interactions between the waste, repository, and surrounding geology
- Simulation of repository-system performance over a 10,000-year period
  - Modeling codes: geophysics, rock mechanics, geohydrology, geochemistry, etc.
  - Utility codes: coordinate transformations, unit conversions, file-format manipulation, etc.
- Consideration of possible future scenarios
  - Undisturbed
  - Human intrusion: mining, drilling

Performance Assessment for WIPP - 2

- **Sources of uncertainty**
  - Modeling uncertainties
  - Variability of physical phenomena (e.g., heterogeneity)
  - Many possible futures
- **Comparison of predicted performance with release limits**
  - Stochastic performance measure
  - Number of simulations dictated by required confidence
- **Large number of complex codes, with complex interactions**
- **Large number of simulations, due to probabilistic nature of problem**



Creep Closure of Repository

Flow of Brine and Gas in the Repository

Direct Releases of Solids Due to Human Intrusion

Transport of Contaminants via Brine and Gas in the Repository

Direct Releases of Fluids Due to Human Intrusion

Generation of Regional Hydraulic Conductivity Fields

Contaminants Removed via Direct Brine Release

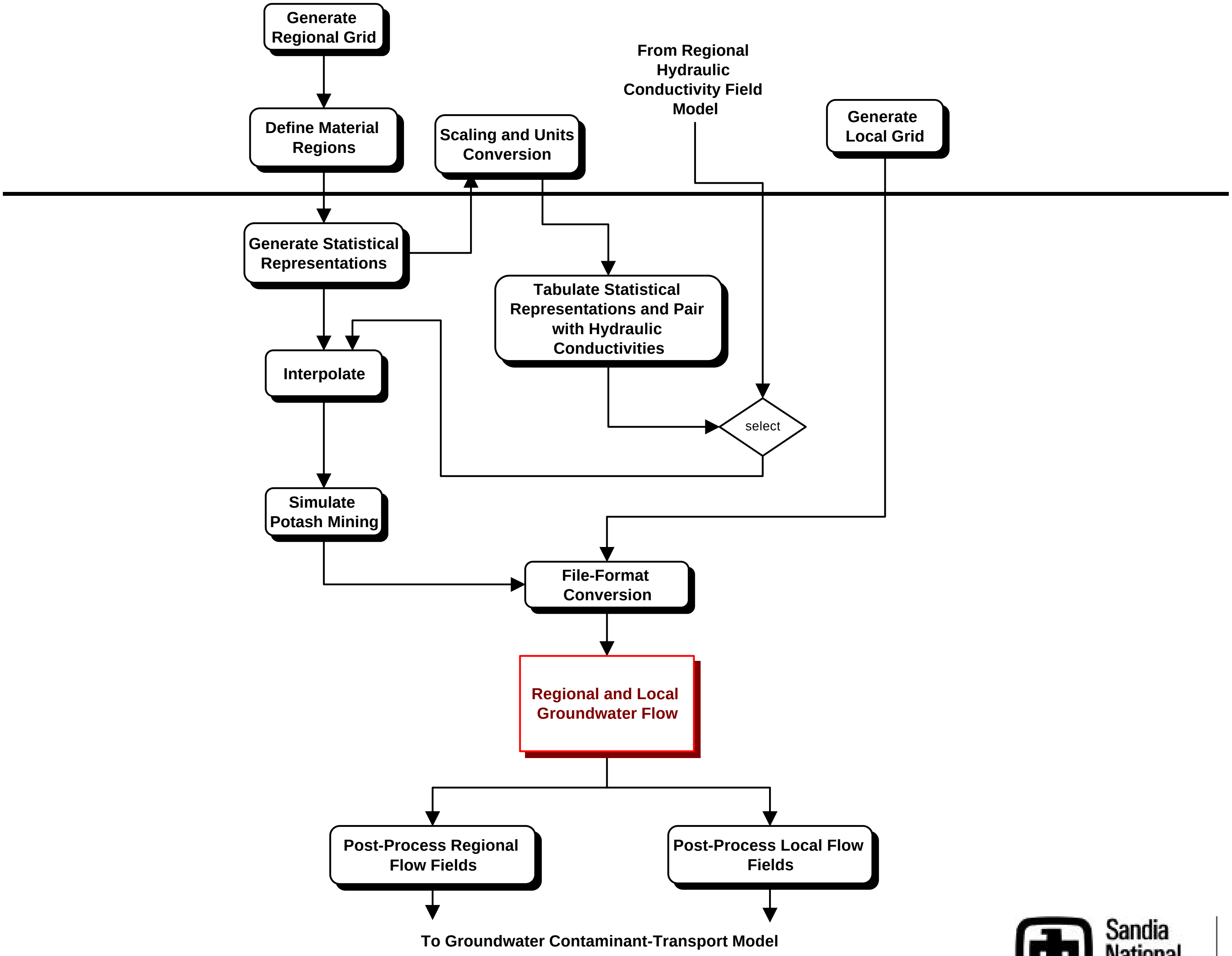
Regional and Local Groundwater Flow

Statistical Combination of All Release Mechanisms

Transport of Contaminants via Groundwater

Output of Compliance Calculation

Sandia National Laboratories


Generate Regional Grid
Define Material Regions
Scaling and Units Conversion
From Regional Hydraulic Conductivity Field Model
Generate Local Grid
Generate Statistical Representations
Tabulate Statistical Representations and Pair with Hydraulic Conductivities
Interpolate
select
Simulate Potash Mining
File-Format Conversion
Regional and Local Groundwater Flow
Post-Process Regional Flow Fields
Post-Process Local Flow Fields
To Groundwater Contaminant-Transport Model

Sandia National Laboratories

The Origins of Our QA Requirements

- **1992 -- Land Withdrawal Act**
  - **EPA named as regulator; made responsible for developing disposal regulations and for certifying long-term safety**
- **Late 1993 -- 40CFR191**
  - **Set forth disposal regulations and release limits**
  - **Told us <u>what</u> we needed to do**
- **Early 1996 -- 40CFR194**
  - **Established criteria for demonstrating compliance with standard 40CFR191**
  - **Invoked NQA 1, 2, and 3**
  - **Told us <u>how</u> we needed to do it**

The Requirements, Summarized

- Our testing, reviews, analyses, and documentation “shall be sufficiently detailed as to purpose, method, assumptions, design input, references, and units such that a person technically qualified in the subject can review and understand the analyses and verify the adequacy of the results without recourse to the originator.”
- We must also provide for software problem reporting, change control, and change tracking

Our Definition of a "High Level of Rigor" -- T^2R^3

- **Traceability: unambiguous identification of all relevant steps and components of a process, along with their sources and linkages**
- **Transparency: clear presentation of the logic and decisions involved in a process**
- **Retrievability: rapid and easy recovery of all relevant components of a process**
- **Reproducibility: reconstruction of a process based on documentation of relevant steps and components to reproduce results**
- **Reliability: establishment of the credibility of each step and component of a process, through reviews**

Application of Our Definition

- Balancing T^2R^3 with cost and schedule
- Application of T^2R^3 principles only to the extent necessary to demonstrate “adequacy of intended use” for the process under consideration
- Recognition that, for WIPP, SNL’s product is the analysis of repository performance and assistance to DOE in the preparation of the Compliance Certification Application (CCA), <u>not</u> software

Where We Began - 1

- Upper-tier requirements derived from DOE Order 5700.6C, <u>but</u> in our implementation:

- No life-cycle methodology
- Inadequate documentation
- No project-wide configuration management
- Poor reproducibility
- Poor traceability
- Inadequate retrievability

Where We Began - 2

- Official QA standards promulgated by 40CFR194, in early 1996 (but rule was proposed in mid-1995)
- Application due October 1996
- Calculation needed to start at beginning of 1996
- Four-month window to revise existing QA Procedures, train staff, and qualify nearly 60 codes! (Serial nature of calculations and SMS helped here)
- In parallel with software QA, there were related activities in qualification of data, analyses, models...

Implementation of Software QA - 1

- Negotiation with DOE and EPA on interpretation of standards -- applying reason
  - Begun after promulgation of 40CFR191, but before 40CFR194 was proposed
  - Negotiated interpretations incorporated into 40CFR194
- Interpretation and applicability of the NQA series, in particular NQA 2.7, to WIPP
  - Vast majority of WIPP codes, developed prior to our use of the standard, exempt from full life cycle (legacy codes -- NQA 2.7, paragraph 10.2)
  - Time-critical problem-response criteria not applicable (e.g., restart capability, unintended function, etc.)
  - Code validation possible only by independent technical review (more aptly regarded as model validation)

Implementation of Software QA - 2

- **Responsibilities divided across teams**
  - **<u>Code Sponsor</u> -- responsible for qualification of a given code; developed functional requirements, most test cases, and related acceptance criteria**
  - **<u>Tester</u> -- performed static and dynamic testing, consulted on test cases, ran all test cases, and compared results to acceptance criteria**
  - **<u>Documentation Support</u> -- prepared all software QA documentation, under the direction of the above team members**
  - **<u>Reviewer(s)</u> -- performed and documented independent technical review of adequacy of testing, and reviewed all software QA documentation**
- **SQA management team periodically reviewed status with individual code teams**

SQA Documentation - 1

- **Requirements Document / Verification and Validation Plan** -- description of code's capabilities and functional requirements; description of test cases needed to test all <u>applicable</u> functional requirements; discussion of acceptance criteria for each test; description of the test procedure to be used, necessary input files, what outputs to expect, etc.
- **User's Manual** -- description of code's capabilities; discussion of theory, models, and numerical methods; instructions for execution; description of input and output files; discussion of limitations and assumptions

SQA Documentation - 2

- **Validation Document** -- description of test results; evaluation of results against acceptance criteria
- **Implementation Document** -- listing of the source code; description of build instructions, compiler directives, libraries linked, and platform; listing of actual build logs; description of code connectivity, e.g., subroutine call tree
- **Design Document** -- description of how to write the code; only required for non-legacy codes (of which there was only 1 in early 1996)

SQA -- Benefits

- Fewer errors due to formal test and review
- Greater reliability of the final product
- Greater defensibility of results
- SQA records to “back up” our results (i.e., to provide objective evidence)

Our Definition of Software Management System (SMS)

The meticulous identification, storage, and ongoing tracking of computer codes from a baseline version through all subsequent versions, along with all relevant inputs, outputs, compilation options, library linkages, and any other information needed to faithfully reproduce the most recent or any previous calculation for which a code has been used (whether for testing or for production)

Implementation of SMS - 1

- Needs identified, software product selected
- Procedures developed, access-control requirements identified
- Three parallel environments provided
  - Development: code sponsors/developers responsible for check-in, check-out, versioning of codes; optional
  - Testing: codes submitted by sponsors for testing, added to software baseline inventory; all official testing performed here
  - Production: once qualified, codes intended for use in official calculations are installed; check-in by authorized SMS administrator <u>only</u>
- Input and output files also under SMS

Implementation of SMS - 2

- Executables built in SMS as well, using build tools
- Rigorous naming conventions enforced
- SQA documentation also in SMS, as well as complete software baseline
- Two additional equivalent, but separate, SMS areas maintained in parallel
  - One for EPA to run the WIPP codes for their own evaluation
  - The other for stakeholders and oversight groups to do likewise
  - Provided appropriate security and T^2R^3 for those groups as well -- proved invaluable!

Our Definition of Run Control

The automated execution of a suite of codes by those granted the necessary access, including retrieval of all needed codes and inputs from within configuration management, and appropriate disposition of outputs, as well as distribution of the computational load across appropriate and/or available resources

Implementation of Run Control

- Leveraged investment in SMS
- All official calculations run by scripts
  - – Codes and inputs pulled from SMS production area
  - – Outputs automatically installed in SMS
  - – Run logs stored in SMS as well
  - – Naming conventions allowed for automatic generation of file names
- All official calculations executed by “run masters”, using only qualified components*
- Also enabled run distribution, for optimum efficiency and use of available resources

*SMS allowed proceeding, at risk, with unqualified codes, to be qualified later

SMS and Run Control -- Benefits 1

- Scalability -- same run scripts can perform 1 or 100,000 runs
- Execution scripts verified only once, and then controlled in SMS
- Reuseability -- never assume a calculation will only be done once!
- Assists in planning and scheduling runs
- Relieves some of the burden from code sponsors (both in conducting calculations and responding to regulator questions about them)

SMS and Run Control -- Benefits 2

- Lessens dependence on specific individuals
- Proper access controls and elimination of manual-interaction steps provides better accuracy and defensibility
- Permits rapid distribution of outputs to analysts

How Well It All Worked - 1

- In May 1998, EPA certified WIPP as being in compliance with the applicable disposal regulations!
- WIPP PA codes were qualified in time
  - Over 40 code sponsors
  - 6-8 testers
  - About 6 documentation support staff
- Massive calculation completed on time, with full T^2R^3
  - Five months end-to-end
  - Conducted by 2 “run masters” (once codes and inputs were qualified and installed in SMS)

How Well It All Worked - 2

- CCA Example
  - 37,000 CPU-hours (over 4.2 CPU-years)
  - 225,000 files retained (many times that number of intermediate results temporarily retained)
  - Approximately 95 Gigabytes in permanent storage
- EPA Example
  - Similar in scope to CCA calculation
  - Conducted by 3 individuals in 3 months for EPA

Lessons Learned - 1

- What worked best
  - Strong management support
  - QA assessments (audits, surveillances)
- Reviewer training
  - Just review adequacy, not coding style
  - Responsibility is merely to answer the question “Is the product adequate for its intended use?”, not “Can I conceive/design a better product?”
- Software QA
  - Implement QA throughout software lifecycle, rather than at end
  - It’s cheaper to *build* in quality than to try to *test* it in

Lessons Learned - 2

- SMS
  - Apply SMS early in software development phase
  - SMS must be consistent and ongoing

- Engage the customer and regulator early -- develop a mutual understanding of requirements and expectations

What Next?

- Increase flexibility and user-friendliness of run control -- DeskTop PA
  - Windows-based interface for scripting calculations
  - Provide automatic traceability and reproducibility
  - Allow for easy substitution of alternative qualified modeling codes
- Expand scope and coverage of electronic CM beyond software -- RDM
  - Center-wide conceptual data model completed
  - Parallel implementation projects underway
  - Expanding capability to cover records, data, models and analyses, project baseline, etc.
  - Integrate with QA procedures

Questions?

Sandia
National
Laboratories